DATE(S) ISSUED:
2/9/2010

SUBJECT:
Security Update of ActiveX Kill Bits (MS10-008)

OVERVIEW:
Microsoft has released a security update which addresses vulnerabilities discovered in multiple ActiveX controls. ActiveX controls are small programs or animations that are downloaded or embedded in Web pages which will typically enhance functionality and user experience. Many web design and development tools have built ActiveX support into their products, allowing developers to both create and make use of ActiveX controls in their programs. There are more than 1,000 existing ActiveX controls available for use today.

When vulnerabilities are discovered in ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Microsoft Internet Explorer includes a security feature which will prevent an ActiveX control from being loaded by using registry settings. This is commonly referred to as setting the 'kill bit' of an ActiveX component. Once the kill bit is set, the associated component can never be loaded.

These vulnerabilities could allow an attacker to take complete control of an affected system. These vulnerabilities may be exploited if a user visits a specifically crafted web page.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

This update will set the kill bits for the following Class Identifier (CLSID):

Office Excel ActiveX control for Data Analysis (max3activex.dll)
CLSID - E0ECA9C3-D669-4EF4-8231-00724ED9288F

Additionally, this update will set the Class Identifier (CLSID) for the following third party software:

Symantec WinFax Pro 10.3
CLSID **-** C05A1FBC-1413-11D1-B05F-00805F4945F6

Google Desktop Gadget v5.8
CLSID - 5D80A6D1-B500-47DA-82B8-EB9875F85B4D

Facebook Photo Updater 5.5.8
CLSID - 0CCA191D-13A6-4E29-B746-314DEE697D83

PandaActiveScan Installer 2.0
CLSID - 2d8ed06d-3c30-438b-96ae-4d110fdc1fb8

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate security update provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-008.mspx
http://www.microsoft.com/technet/security/bulletin/ms09-055.mspx
http://www.microsoft.com/technet/security/bulletin/ms09-035.mspx
http://www.microsoft.com/technet/security/bulletin/ms09-032.mspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0252